The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/27/2016
12/29/2016 - UPDATED

SUBJECT:
A Vulnerability in PHPMailer Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in PHPMailer, which could result in remote code execution. PHPMailer is a very popular library for PHP that allows for the sending of emails. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the web server user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If the webserver has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild, however proof of concept code has been published.

SYSTEMS AFFECTED:

- PHPMailer versions prior to 5.2.18

December 29 - UPDATED **SYSTEMS AFFECTED:**

- **PHPMailer versions prior to 5.2.21**

RISK:
Government:

- Large and medium government entities: **High**
- Small government: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in PHPMailer, which could result in remote code execution. This vulnerability can be exploited by targeting common components of websites such as contact forms, feedback forms, registration forms, password and email reset forms, and other forms. This vulnerability has been assigned CVE-2016-10033.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the web server user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If the webserver has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative user rights.

December 29 - UPDATED TECHNICAL SUMMARY:

A bypass to the patch assigned to fix the previously released vulnerability was released as CVE-2016-10045, which could also allow for remote code execution. The latest version of PHPMailer, 5.2.21, addresses this bypass.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the latest version of PHPMailer immediately, after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all systems and services.

REFERENCES:

Legalhackers:

http://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html

PHPMailer:

https://github.com/PHPMailer/PHPMailer/releases/tag/v5.2.18

Securityfocus:

http://www.securityfocus.com/bid/95108

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10033

December 29 - UPDATED REFERENCES:

Legalhackers:

https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10045-Vuln-Patch-Bypass.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10045